ÁLGEBRA LINEAL Y ESTRUCTURAS MATEMÁTICAS

5 de Noviembre de 2019

Alumno:_____ **D.N.I.:**_____ **Grupo F**

Ejercicio 1. *Sean* $x = 3210)_4$, $y = 135)_8$. *Calcula la expresión en hexadecimal de* $x + 2y$, xy *y* $x - y$ *(no se puede realizar ningún cálculo en base* 10*).*

Solución:

Vamos a expresar x e y en binario. Puesto que x está en base $4 = 2^2$ e y está en base $8 = 2^3$, podemos pasarlo a binario cifra a cifra:

$$x = 3210)_4 = 11100100)_2; \qquad y = 135)_8 = 1011101)_2.$$

Para calcular $2y$, y puesto que $2 = 10)_2$, añadimos un cero a la derecha de la expresión binaria de y. Es decir, $2y = 10111010)_2$.

Calculamos $x + 2y$ y xy.

$$\begin{array}{cccccccc} & {\scriptstyle 1} & {\scriptstyle 1} & & & & & \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}$$

$$\begin{array}{cccccccccccccccc} & & & & & & & & & & & & & {\scriptstyle 1} & {\scriptstyle 1} & \\ & & & & & & & & & & & & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ & & & & & & & & & & & & & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline & & & & & & & & & & & {\scriptstyle 1} & {\scriptstyle 1} & & & & & & & \\ & & & & & & & & {\scriptstyle 10} & {\scriptstyle 1} & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ & & & & & & & {\scriptstyle 10} & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & & \\ & & & & & & {\scriptstyle 10} & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & & & \\ & & & & & {\scriptstyle 1} & {\scriptstyle 10} & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & & & & \\ & & & & & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & & & & & & \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}$$

Y para calcular $x - y$ utilizamos la representación en complemento a 2. Para escribir $-y$, le añadimos a y un cero a la izquierda, intercambiamos ceros y unos, y sumamos uno.

$$1011101 \longrightarrow 01011101 \longrightarrow 10100010 \longrightarrow 10100011$$

Y ahora efectuamos la suma:

$$\begin{array}{cccccccccc} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & & & & & \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}$$

Eliminamos el 1 del acarreo final, por lo que nos queda que el número $x - y$ es 010000111. Al empezar por 0 dicho número es positivo, y en binario se escribe $x - y = 10000111)_2$.

Ya tenemos $x + 2y$, xy y $x - y$ en binario. Para expresarlos en hexadecimal agrupamos las cifras de cuatro en cuatro, empezando por la derecha y pasamos cada uno de esos grupos a una cifra hexadecimal:

$$x + 2y = 110011110)_2 = 19E)_{16}; \quad xy = 101001011010100)_2 = 52D4)_{16}; \quad x - y = 10000111)_2 = 87)_{16}.$$

Ejercicio 2. *De un número natural x sabemos que:*

- *Si le restamos* 3 *es múltiplo de* 8 *y de* 14*.*
- *Su triple da resto* 12 *al dividirlo por* 13*.*
- *Si le sumamos* 1*, la suma de sus cifras vale* 4*.*
- *Es menor que* 8000*.*

¿Cuál es el número x?

Solución:
Traducimos las tres primeras condiciones a congruencias:

- Esto significa que $x \equiv 3$ mód 8 y $x \equiv 3$ mód 14. También se podría decir que $x - 3$ es múltiplo del mínimo común múltiplo de 8 y 14, es decir, de 56, y traducirlo como $x \equiv 3$ mód 56.
- En este caso tenemos $3x \equiv 12$ mód 13.
- Puesto que el resto de dividir un número entre 9 es lo mismo que el resto de dividir la suma de sus cifras entre 9, esta condición la podemos expresar como $x + 1 \equiv 4$ mód 9, o si queremos, $x \equiv 3$ mód 9.

Con esto, nuestro número x debe ser una solución del siguiente sistema de congruencias:

$$\begin{array}{rcrcr} x & \equiv & 3 & \text{mód} & 8 \\ x & \equiv & 3 & \text{mód} & 14 \\ 3x & \equiv & 12 & \text{mód} & 13 \\ x & \equiv & 3 & \text{mód} & 9 \end{array}$$

Resolvemos ahora el sistema. Comenzamos por la primera congruencia:

$x \equiv 3$ mód 8	Escribimos la forma de la solución.
$x = 3 + 8k_1 : \ k_1 \in \mathbb{Z}$	Sustituimos en la segunda.
$3 + 8k_1 \equiv 3$ mód 14	Operamos.
$8k_1 \equiv 0$ mód 14	$\text{mcd}(8, 14) = 2$. Dividimos por 2.
$4k_1 \equiv 0$ mód 7	Multiplicamos por $4^{-1} = 2$.
$k_1 \equiv 0$ mód 7	Escribimos cuánto vale k_1.
$k_1 = 7k_2 : \ k_2 \in \mathbb{Z}$	Sustituimos en $x = 3 + 8k_1$.
$x = 3 + 8k(7k_2) = 3 + 56k_2$	Sustituimos en la tercera congruencia.
$3(3 + 56k_2) \equiv 12$ mód 13	Operamos.
$9 + 168k_2 \equiv 12$ mód 13	
$168k_2 \equiv 3$ mód 13	Reducimos módulo 13.
$12k_2 \equiv 3$ mód 13	Multiplicamos por 12^{-1}mód $13 = 12$.
$144k_2 \equiv 36$ mód 13	Reducimos módulo 13.
$k_2 \equiv 10$ mód 13	Escribimos cuánto vale k_2.
$k_2 = 10 + 13k_3 : \ k_3 \in \mathbb{Z}$	Sustituimos k_2 en $x = 3 + 56k_2$.
$x = 3 + 56(10 + 13k_3) = 563 + 728k_3$	Sustituimos en la cuarta congruencia.
$563 + 728k_3 \equiv 3$ mód 9	Operamos.
$728k_3 \equiv -560$ mód 9	Reducimos módulo 9.
$8k_3 \equiv 7$ mód 9	Multiplicamos por 8^{-1}mód $9 = 8$.
$64k_3 \equiv 56$ mód 9	Reducimos módulo 9.
$k_3 \equiv 2$ mód 9	Escribimos el valor de k_3.
$k_3 = 2 + 9k : \ k \in \mathbb{Z}$	Sustituimos en $x = 563 + 728k_3$ y operamos.
$x = 563 + 728(2 + 9k) = 2019 + 6552k$	

Y ya tenemos la solución del sistema de congruencias. Es $x = 2019 + 6552k : k \in \mathbb{Z}$. Podemos ver que la única solución positiva y menor que 8000 se da cuando $k = 0$, en cuyo caso tenemos $x = 2019$. Este es el número que buscábamos.

Si la última condición no logramos expresarla como una congruencia, tendríamos que resolver el sistema formado por las tres primeras. La solución de este sistema es $x = 563 + 728k_3$. Y las soluciones que hay menores que 8000 son:

$x = 563$; $x = 1291$; $x = 2019$; $x = 2747$; $x = 3475$; $x = 4203$; $x = 4931$; $x = 5659$; $x = 6387$; $x = 7115$; $x = 7843$.

Y de estos valores, el único que al sumarle uno da un número cuyas cifras suman 4 es 2019.

Notemos por último que las congruencias primera, seguna y cuarta nos dicen que el número $x-3$ es múltiplo de 8, 14 y 9, y puesto que $\text{mcm}(8,14,9) = 504$, la solución de estas tres congruencias es $x = 3 + 504k : k \in \mathbb{Z}$. Esto simplifica mucho la resolución del sistema.

Ejercicio 3. *Dada la ecuación diofántica* $37x - 29y = 11$*, se pide:*

1. *¿Cuántas soluciones tiene en las que* x *está comprendido entre* 0 *y* 10000*?*
2. *¿En cuántas de ellas, además,* y *está también entre* 0 *y* 10000*?*
3. *Y, ¿en cuántas de ellas* x *es múltiplo de* 5*?*

Solución:
Para resolver la ecuación diofántica, en primer lugar la expresamos como una congruencia:

$$37x \equiv 11 \text{ mód } 29.$$

O lo que es lo mismo, $8x \equiv 11$ mód 29. Calculamos el inverso de 8 módulo 29.

29		0
8		1
5	3	v_1
3	1	v_2
2	1	v_3
1	1	v_4

$v_1 = 0 - 3 \cdot 1 = -3$
$v_2 = 1 - 1 \cdot (-3) = 4$
$v_3 = -3 - 1 \cdot 4 = -7$
$v_4 = 4 - 1 \cdot (-7) = 11$

29		0
8		1
5	3	-3
3	1	4
2	1	-7
1	1	11

El inverso vale 11, luego multiplicamos por 11, y nos queda $x \equiv 121$ mód 29, y como $121 = 4 \cdot 29 + 5$ reducimos y tenemos $x \equiv 5$ mód 29.

La solución de la congruencia es $x = 5 + 29k : \ k \in \mathbb{Z}$. Sustituimos en la ecuación incial y despejamos y.

$37(5 + 29k) - 29y = 11.$
$185 + 37 \cdot 29k - 11 = 29y.$
$29y = 174 + 37 \cdot 29k.$
$y = \frac{174+37\cdot 29k}{29} = 6 + 37k.$

Luego la solución de la ecuación diofántica es:

$$\begin{array}{rcrcl} x & = & 5 & + & 29k \\ y & = & 6 & + & 37k \end{array} \qquad k \in \mathbb{Z}$$

Y ahora, para resolver los apartado 1 y 2 planteamos las desigualdades $0 \leq x \leq 10000$ y $0 \leq y \leq 10000$.

$$\begin{array}{ccccc} 0 & \leq & 5 + 29k & \leq & 10000 \\ -5 & \leq & 29k & \leq & 9995 \\ \frac{-5}{29} & \leq & k & \leq & \frac{9995}{29} \\ -0'17 & \leq & k & \leq & 344'65 \\ 0 & \leq & k & \leq & 344 \end{array} \qquad \begin{array}{ccccc} 0 & \leq & 6 + 37k & \leq & 10000 \\ -6 & \leq & 37k & \leq & 9994 \\ \frac{-6}{37} & \leq & k & \leq & \frac{9994}{37} \\ -0'16 & \leq & k & \leq & 270'1 \\ 0 & \leq & k & \leq & 270 \end{array}$$

Para que x esté entre 0 y 10000, k debe estar entre 0 y 344. Hay entonces 345 soluciones.

Si además queremos que y esté entre 0 y 10000, entonces k debe estar entre 0 y 270. Hay entonces 271 soluciones.

Por último, si además x debe ser múltiplo de 5 lo que tenemos es $5 + 29k \equiv 0$ mód 5. Esta congruencia es equivalente a $k \equiv 0$ mód 5 cuya solución es $k = 5k'$.

Tenemos entonces $k = 5k'$ y $0 \leq k \leq 270$. Eso se traduce en $0 \leq k' \leq 54$. Hay por tanto 55 soluciones en las que x e y están entre 0 y 10000 y además x es múltiplo de 5.

Ejercicio 4. *Sea* $A = \mathbb{Z}_3[x]_{x^3+2x^2+x+2}$.

1. *¿Cuántos elementos tiene A?*
2. *¿Es A un cuerpo?*
3. *Calcula en A, si es posible,* $(x^2+x+1)(2x^2+x+2)$ *y* $(2x^2+x+1)^{-1}$.
4. *Encuentra, si es posible, un elemento* $\alpha \in A$ *tal que*

$$(\alpha + x^2)(2x+2) = \alpha(x+2)^2.$$

Solución:

1. El número de elementos de A es $3^3 = 27$. Se corresponden con los polinomios, con coeficientes en $\mathbb{Z}_3$ de grado menor que 3 (y el polinomio cero).

2. Para que A sea un cuerpo el polinomio $m(x) = x^3+2x^2+x+2$ debe ser irreducible. Pero $m(1) = 0$, lo que nos dice que $x - 1 = x + 2$ es un divisor de $m(x)$. Por tanto, A no es un cuerpo.

3. Calculamos en primer lugar la multiplicación:

$$\begin{array}{ccccc} & & 1 & 1 & 1 \\ & & 2 & 1 & 2 \\ \hline & & 2 & 2 & 2 \\ & 1 & 1 & 1 & \\ 2 & 2 & 2 & & \\ \hline 2 & 0 & 2 & 0 & 2 \end{array}$$

Vemos que $(x^2+x+1)(2x^2+x+2) = 2x^4+2x^2+2$. Reducimos ahora módulo $m(x)$.

$$\begin{array}{c|ccccc} & 2 & 0 & 2 & 0 & 2 \\ 1 & & 2 & 2 & & \\ 2 & & & 1 & 1 & \\ 1 & & & & 2 & 2 \\ \hline & 2 & 2 & 2 & 0 & 1 \end{array}$$

El resto de la división es $2x^2+1$. Por tanto, $(x^2+x+1)(2x^2+x+2) = 2x^2+1$.

Para calcular $(2x^2+x+1)^{-1}$ nos valemos del algoritmo extendido de Euclides.

$$\begin{array}{c|cccc} 2 & 1 & 2 & 1 & 2 \\ \hline 1 & & 1 & 0 & \\ 1 & & & 1 & 0 \\ \hline & 1 & 0 & 2 & 2 \end{array} \qquad \begin{array}{l} c(x) = 2x \\ \\ r(x) = 2x+2 \end{array} \qquad \begin{array}{c|ccc} 2 & 2 & 1 & 1 \\ \hline 2 & & 1 & 1 \\ \hline & 2 & 2 & 2 \end{array} \qquad \begin{array}{l} c(x) = 2(2x+2) = x+1 \\ \\ r(x) = 2 \end{array}$$

Con esta última división vemos que $\mathrm{mcd}(x^3+2x^2+x+2, 2x^2+x+1) = 1$ y por tanto, el inverso existe.

x^3+2x^2+x+2		0
$2x^2+x+1$		1
$2x+2$	$2x$	$v_1(x)$
2	$x+1$	$v_2(x)$
1		$2v_2(x)$

x^3+2x^2+x+2		0
$2x^2+x+1$		1
$2x+2$	$2x$	x
2	$x+1$	$2x^2+2x+1$
1		x^2+x+2

$v_1(x)$ y $v_2(x)$ se han calculado como sigue: $v_1(x) = 0 - 1 \cdot 2x = x$ y $v_2(x) = 1 - (x+1)x = 1 + 2x(x+1) = 2x^2+2x+1$.

Tenemos entonces que $(2x^2+x+1)^{-1} = x^2+x+2$.

4. Para resolver la ecuación $(\alpha + x^2)(2x + 2) = \alpha(x + 2)^2$ operamos y llevamos al miembro de la izquierda todos los términos que tienen α y a la derecha el resto. Y después despejamos α.

   $(\alpha + x^2)(2x + 2) = \alpha(x + 2)^2$
   $\alpha(2x + 2) + x^2(2x + 2) = \alpha(x^2 + 4x + 4)$
   $\alpha(2x + 2) + x^2(2x + 2) = \alpha(x^2 + x + 1)$
   $\alpha(2x + 2) - \alpha(x^2 + x + 1) = -x^2(2x + 2)$
   $\alpha(2x + 2 - x^2 - x + 1) = 2x^2(2x + 2)$
   $\alpha(2x + 2 + 2x^2 + 2x + 2) = x^3 + x^2$
   $\alpha(2x^2 + x + 1) = x^3 + x^2$
   $\alpha = (x^3 + x^2)(2x^2 + x + 1)^{-1}$
   $\alpha = (x^3 + x^2)(x^2 + x + 2)$
   $\alpha = x^5 + x^4 + 2x^3 + x^4 + x^3 + 2x^2$
   $\alpha = x^5 + 2x^4 + 2x^2$
   $\alpha = 2x^2 + x + 2$

   Donde el último resultado se ha obtenido de la igualdad

   $$x^5 + 2x^4 + 2x^2 = (x^3 + 2x^2 + x + 2)(x^2 + 2) + (2x^2 + x + 2),$$

   que viene de la división siguiente:

	1	2	0	2	0	0
1		1	0	2		
2			2	0	1	
1				1	0	2
	1	0	2	2	1	2

   Podemos ver que $\alpha + x^2 = x + 2$, luego $(\alpha + x^2)(2x + 2) = (x + 2)(2x + 2) = 2x^2 + 1$.

   Por otra parte, $\alpha(x+2)^2 = (2x^2+x+2)(x^2+x+1) = 2x^2+1$, como vimos en el apartado anterior.

Ejercicio 5. *Sea* $m(x) = x^7+x^6+x^5+2x^4+x^3+2x^2+2x+1 \in \mathbb{Z}_3[x]$ *y* $q(x) = x^5+2x^4+2x^3+x+1 \in \mathbb{Z}_3[x]$.

1. *Calcula* $mcd(m(x), q(x))$.
2. *Factoriza* $m(x)$ *como producto de irreducibles.*

Solución:

1. *Hacemos las divisiones correspondientes para calcular el máximo común divisor:*

	1	1	1	2	1	2	2	1
1		1	2	1				
1			1	2	1			
0				0	0	0		
2					2	1	2	
2						2	1	2
	1	2	1	2	1	2	2	0

$c(x) = x^2 + 2x + 1$
$r(x) = 2x^4 + x^3 + 2x^2 + 2x$

2	1	2	2	0	1	1
1		1	0			
2			2	0		
2				2	0	
0					0	0
	1	0	1	2	1	1

$c(x) = 2 \cdot x$
$r(x) = x^3 + 2x^2 + x + 1$

	2	1	2	2	0
1		2	0		
2			1	0	
2				1	0
	2	0	0	0	0

$c(x) = 2x$
$r(x) = 0$

Como el último resto no nulo es x^3+2x^2+x+1 *concluimos que* $mcd(m(x), q(x)) = x^3+2x^2+x+1$.

2. *Ya tenemos un divisor de* $m(x)$ *(lo hemos obtenido en el apartado anterior). Dividimos* $m(x)$ *entre* $x^3 + 2x^2 + x + 1$.

	1	1	1	2	1	2	2	1
1		1	2	2	1	1		
2			2	1	1	2	2	
2				2	1	1	2	2
	1	2	2	1	1	0	0	0

Y tenemos que $m(x) = (x^3 + 2x^2 + x + 1)(x^4 + 2x^3 + 2x^2 + x + 1)$. *Ahora factorizamos cada uno de estos dos polinomios.*

- $q_1(x) = x^3 + 2x^2 + x + 1$. *Por ser de grado* 3 *sólo tenemos que ver si tiene o no raíces:* $q_1(0) = 1 \neq 0$, $q_1(1) = 1+2+1+1 = 2 \neq 0$, $q_1(2) = 2^3+2\cdot 2^2+2+1 = 8+8+2+1 = 1 \neq 0$. *Como no tiene raíces,* $q_1(x)$ *es irreducible.*
- $q_2(x) = x^4 + 2x^3 + 2x^2 + x + 1$. *Comprobamos si tiene raíces:* $q_2(0) = 1 \neq 0$, $q_2(1) = 1+2+2+1+1 = 1 \neq 0$, $q_2(2) = 2^4+2\cdot 2^3+2\cdot 2^2+2+1 = 43 = 1 \neq 0$. *Este polinomio tampoco tiene raíces, pero al ser de grado* 2 *hemos de probar por los irreducibles de grado* 2.

$x^2 + 1$

	1	2	2	1	1
0		0	0	0	
2			2	1	2
	1	2	1	2	0

$c(x) = x^2 + 2x + 1$
$r(x) = 2x$

$x^2 + x + 2$

	1	2	2	1	1
2		2	2	1	
1			1	1	2
	1	1	2	0	0

$c(x) = x^2 + x + 2$
$r(x) = 0$

Y vemos que $x^4 + 2x^3 + 2x^2 + x + 1 = (x^2 + x + 2)^2$.

Por tanto, la factorización de $m(x)$ *como producto de irreducibles es:*

$$m(x) = (x^2 + x + 2)^2 \cdot (x^3 + 2x^2 + x + 1).$$